CBI
Ministry of Foreign Affairs

What requirements must outsourcing services comply with for the European market?

Service providers wanting to enter the European outsourcing market have to comply with several requirements. The main legal requirements concern the protection of copyright and personal data. Important additional requirements are the presence of a quality management system and effective data security measures. In Northern and Western Europe, Corporate Social Responsibility policies and environmentally friendly practices are becoming increasingly important.

Contents of this page

1 . What legal and non-legal requirements must your product/service comply with?

Copyright

Legal protection of computer programs

The European Union has established specific rules to protect computer programs by means of copyright.

The Directive on the legal protection of computer programs (2009/24/EC) establishes that:

- you have to make sure not to breach any copyright when placing your computer program on the market
- your products are also protected against unauthorised reproduction

Tips:

- Read more on the legal protection of computer programs on the website of the European Commission.
- All European Union member states have implemented the European Directive into national legislation. Although they are generally the same, you should check the exact regulations in your European target market.

Personal data protection

Privacy is highly protected in Europe. The European Union has several directives in place for this purpose. Providers that do not respect these directives may be subject to enforcement actions and/or possible claims - even if they are located outside Europe.

General Data Protection Regulation

The new General Data Protection Regulation (GDPR) came into effect on 25 May 2018. This regulation is designed to protect individuals in Europe from privacy and data breaches. It is also being incorporated into the EEA-Agreement with Iceland, Liechtenstein, Norway and Switzerland.

These new rules were introduced to give people more control over their personal data and let businesses benefit from a level playing field. The GDPR applies to all companies processing the personal data of individuals in Europe, regardless of the company's location. This means it also applies to you directly.

Under the old directive, the protection of any data by which an individual can be identified was the sole responsibility of the data controller (owner). However under the GDPR, any company or individual that processes data is also responsible for its protection. The personal data this regulation protects can range from a name or email address, to bank details, social media content, a photo or an IP address, among other data.

Some key consumer rights you must comply with include, but are not limited to:

- consent — consumers must explicitly consent by opting in, consent must be easy to withdraw and requests must be specific and in plain language;
- right to access — consumers are entitled to know whether or not companies process their personal data, where and for what purpose;
- data portability — consumers are entitled to a copy of their personal data, free of charge, in a commonly used and machine-readable format;
- right to be forgotten — consumers are entitled to have their personal data erased and have processing and further dissemination halted;
- privacy by design — data protection should be included from the onset of designing systems, data should be minimised and access limited.

e-Privacy Directive

The ePrivacy Directive (2002/58/EC), commonly known as the 'cookie law', contains specific regulations for data protection in the electric communications sector.

For instance:

- Sending unsolicited commercial electronic messages ('spam') is not allowed.
- There are strict rules on the use of cookies.
- Contact details may only be published with the consent of the subject.

A new ePrivacy Regulation was originally scheduled to enter into force along with the GDPR, but its implementation has since been delayed. The new regulation is intended to safeguard the confidentiality of electronic communications through stronger privacy rules. Unlike the current directive, it includes Internet-based voice and Internet-messaging technologies such as Skype, WhatsApp and Facebook Messenger.

Tips:

- Note that the legislation on data protection is only relevant if your services involve personal data.
- If you are dealing with personal data, study the GDPR's new European data protection rules and principles, for a good understanding of what is allowed and what is not.

- Audit your current data to determine whether it is GDPR compliant. What data do you have, where and why? Did you or your client obtain explicit consent to use it for this specific purpose?
- Do not collect or store more information about your or your client's customers than strictly necessary.
- Set up clear consent request forms and privacy policies that inform your and your client's customers how you process their personal data. For more information, see the GDPR consent guidance from the UK's Information Commissioner's Office and Econsultancy's GDPR: How to create best practice privacy notices (with examples).
- Keep records of your obtained consent.
- Be aware of what data you store and where, to be able to comply with potential consumer requests.
- Make sure your staff is aware of your policy, so they do not unintentionally violate GDPR regulations.
- To determine how compliant you are and what you may need to improve, try IDC's GDPR Readiness Assessment.
- Read more on digital privacy on the website of the European Commission. This is also where you can keep up to date on the reforms of the European ePrivacy rules.
- Contact Open Trade Gate Sweden if you have specific questions regarding rules and requirements in Sweden and the European Union.

2 . What additional requirements do buyers often have?

Quality management

Many European buyers only do business with companies that have a quality management system in place. Such a system shows that you are well organised and able to deliver the required service quality. There are several common options.

ISO 9001:2015

The best-known quality management standard is ISO 9001:2015. It aims to ensure that you can give your customers consistent, good quality products and services. If you comply with ISO 9001:2015 you can obtain certification, but this is not a requirement.

Capability Maturity Model Integration

Another option is the Capability Maturity Model Integration (CMMI), which has been adopted worldwide. You can achieve a 1-5 maturity level rating, indicating your improvement in multiple process areas. CMMI Services helps you to improve your capability to provide your customers with quality services.

Sector-specific standards

European buyers often require you to comply with a sector-specific standard or code of practice (if available).

Examples are:

- Basel II and Basel III - finance and banking
- HL7 - healthcare

- PCI DSS - payment cards
- COPC or ISO 18295-1:2017 - contact centres
- Code of Practice for Cloud Service Providers - cloud computing

Tips:

- Implement ISO 9001 or CMMI (maturity level 3-5). These are the most commonly used quality management systems in the outsourcing market. Even if you have developed a good in-house quality management system, buyers prefer a system they recognise.
- Buyers expect you to know which standards are relevant for the services you provide. Do your research in advance, so you can show them your company complies with these standards.
- Check which sector-specific standards or codes are available for your specific product, for example by asking your sector association or your buyer. Also ask your buyer to what extent they want you to implement these standards.

Security

Data security is one of the main challenges for service providers. This includes both data protection and recovery systems. Many European buyers expect you to implement an information security and management system, especially in industries in which security is essential, such as finance and banking or mobile applications. The ISO 27000-series contains common standards for information security.

Tips:

- Make sure you have effective security processes and systems in place, from business continuity and disaster recovery to virus protection.
- Ask your buyer to what extent they require you to implement a security management system like ISO 27002.

Corporate Social Responsibility

Corporate Social Responsibility (CSR) refers to companies taking responsibility for their impact on society. It makes companies more sustainable and ‘green’.

Socially responsible companies pay attention to the following concerns in their policy:

- social
- environmental
- ethical
- consumer and human rights

CSR is becoming especially important to large companies and governments in Northern and Western Europe. Many European companies involve their suppliers in their CSR policies. In the future, CSR may well become a direct selection criterion. Having a well-documented CSR policy may therefore give you a competitive advantage over companies without one. ISO 26000 provides guidance on CSR.

Tips:

- Read more about Corporate Social Responsibility in practice on the website of the European Commission.
- Show that you care about your impact on society and the environment by implementing your own CSR policy. It can be a unique selling point (USP) when your buyer has to select a service provider.
- Clearly communicate your commitment to CSR and the environment in your marketing activities.

For a full overview of certification schemes in the outsourcing sector, you can consult ITC Standards Map.

Please review our market information disclaimer.

Follow us for the latest updates

Twitter

Facebook

LinkedIn

RSS